日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年１１月１９日
出願番号 Application Number: [ST. 10/C]:	特願２００３－３８９２３０ [ＪＰ２００３－３８９２３０]
出願人 Applicant(s):	株式会社日立製作所

U.S. Appln. Filed 2-26-04
Inventor: Y. Ishii et al
mattingly stanger & malur
Docket MEI-101

２００４年　２月　３日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３００５３１３

【書類名】　特許願
【整理番号】　PA20G215
【提出日】　平成15年11月19日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　石井　陽介
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　薗田　浩二
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　岩嵜　正明
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社日立製作所
【代理人】
　【識別番号】　110000028
　【氏名又は名称】　特許業務法人　明成国際特許事務所
　【代表者】　下出　隆史
　【電話番号】　052-218-5061
【手数料の表示】
　【予納台帳番号】　133917
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0111082

【書類名】特許請求の範囲
【請求項１】
ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、
前記ネットワークには、前記ストレージ装置および前記アクセス制御装置が複数接続されており、
該アクセス制御装置は、
各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、
前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限するアクセス制限部と、
アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける情報入力部と、
前記入力に基づき、前記ネットワークに接続された各アクセス制御装置がそれぞれ参照する前記アクセス禁止リストを更新する処理を行うリスト更新部とを備えるアクセス制御装置。
【請求項２】
請求項１記載のアクセス制御装置であって、
前記リスト更新部は、前記他のアクセス制御装置に対して、前記ユーザ情報を該他のアクセス制御装置が参照する前記アクセス禁止リストに登録させる登録指示を配信するアクセス制御装置。
【請求項３】
請求項１記載のアクセス制御装置であって、
前記リスト更新部は、前記更新された前記アクセス禁止リストを、前記他のアクセス制御装置へ配信するアクセス制御装置。
【請求項４】
ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、
前記ネットワークには、前記ストレージ装置および前記アクセス制御装置が複数接続されており、
各情報資源のアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、
前記ネットワークに接続された他のアクセス制御装置から、前記各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する受信部と、
前記所定の情報により、前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストを更新するリスト更新部と、
前記アクセスコントロールリストより前記アクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えるアクセス制御装置。
【請求項５】
請求項１～請求項４いずれか記載のアクセス制御装置であって、
前記アクセス制限部は、未完了の処理を含めて、前記アクセス制限を行うアクセス制御装置。
【請求項６】
請求項１～請求項５いずれか記載のアクセス制御装置であって、
前記アクセス禁止リストに基づき、前記アクセスコントロールリストを更新するアクセスコントロールリスト更新部を備えるアクセス制御装置。
【請求項７】
請求項６記載のアクセス制御装置であって、
前記アクセス禁止リスト内のユーザ情報を、所定のタイミングで削除するアクセス制御装置。
【請求項８】

請求項７記載のアクセス制御装置であって、
前記所定のタイミングとは、前記アクセスコントロールリスト更新部における前記更新の終了後であるアクセス制御装置。
【請求項９】
請求項７記載のアクセス制御装置であって、
前記所定のタイミングとは、前記ネットワークに接続された全てのアクセス制御装置における、前記アクセスコントロールリスト更新部における前記更新の終了後であるアクセス制御装置。
【請求項１０】
情報資源を格納するストレージ装置と、情報資源のアクセスを制御するためのアクセス制御装置とが、ネットワークに複数接続されたアクセス制御システムであって、
各アクセス制御装置は、
各情報資源へのアクセス許否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、
前記アクセスコントロールリストより、前記情報資源へのアクセスを禁止すべきユーザを特定可能な所定の情報を登録したアクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えており、
いずれか一のアクセス制御装置は、自装置が参照する前記アクセス禁止リストに変更が発生した場合に、前記所定の情報、または、前記アクセス禁止リストを、前記ネットワークに接続された他のアクセス制御装置に配信する配信部を備え、
前記他のアクセス制御装置は、前記所定の情報、または、前記アクセス禁止リストを受信し、自装置が参照するアクセス禁止リストを更新するリスト更新部を備えるアクセス制御システム。
【請求項１１】
請求項１０記載のアクセス制御システムであって、
前記配信部は、前記他のアクセス制御装置へ、前記アクセス禁止リストを更新するための更新情報を同報配信するアクセス制御システム。
【請求項１２】
請求項１０記載のアクセス制御システムであって、
前記アクセス禁止リストを更新するための更新情報を最初に配信するアクセス制御装置の前記配信部は、前記アクセス禁止リストを更新するための更新情報を、予め設定された他のアクセス制御装置へ配信し、
前記他のアクセス装置の配信部は、受信した前記更新情報を、更に、予め設定された他のアクセス制御装置へ配信するアクセス制御システム。
【請求項１３】
ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御方法であって、
前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されており、
各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う工程と、
前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限する工程と、
アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける工程と、
前記入力に基づき、前記ネットワークに接続された各アクセス制御装置がそれぞれ参照する前記アクセス禁止リストを更新する処理を行う工程とを備えるアクセス制御方法。
【請求項１４】
ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御方法であって、
前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されて

おり、
　各情報資源のアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う工程と、
　前記ネットワークに接続された他のアクセス制御装置から、前記各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する工程と、
　前記所定の情報により、前記アクセス禁止リストを更新する工程と、
　前記アクセスコントロールリストより前記アクセス禁止リストを優先してアクセスを制限する工程とを備えるアクセス制御方法。
【請求項１５】
　情報資源を格納するストレージ装置と、該オブジェクトへのアクセスを制御するためのアクセス制御装置とが、ネットワークに複数接続されたアクセス制御システムにおいてアクセスを制御するアクセス制御方法であって、
　各アクセス制御装置は、
　各情報資源へのアクセス許否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、
　前記アクセスコントロールリストより、前記情報資源へのアクセスを禁止すべきユーザを特定可能な所定の情報を登録したアクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えており、
　いずれか一のアクセス制御装置は、自装置が参照する前記アクセス禁止リストに変更が発生した場合に、前記所定の情報、または、前記アクセス禁止リストを、前記ネットワークに接続された他のアクセス制御装置に配信する工程を備え、
　前記他のアクセス制御装置は、前記所定の情報、または、前記アクセス禁止リストを受信し、自装置が参照するアクセス禁止リストを更新する工程を備えるアクセス制御方法。
【請求項１６】
　ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスをコンピュータに制御させるためのコンピュータプログラムであって、
　前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されており、
　各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う機能と、
　前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限する機能と、
　アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける機能と、
　前記入力に基づき、前記ネットワークに接続された各アクセス制御装置がそれぞれ参照する前記アクセス禁止リストを更新する処理を行う機能とをコンピュータに実現させるためのコンピュータプログラム。
【請求項１７】
　ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスをコンピュータに制御させるためのコンピュータプログラムであって、
　前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されており、
　各情報資源のアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う機能と、
　前記ネットワークに接続された他のアクセス制御装置から、前記各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する機能と、
　前記所定の情報により、前記アクセス禁止リストを更新する機能と、
　前記アクセスコントロールリストより前記アクセス禁止リストを優先してアクセスを制限する機能とをコンピュータに実現させるためのコンピュータプログラム。
【請求項１８】
　請求項１６または請求項１７記載のコンピュータプログラムをコンピュータ読み取り可

能に記録した記録媒体。

【書類名】明細書
【発明の名称】ブラックリストによる緊急アクセス遮断装置
【技術分野】
【０００１】
本発明は、コンピュータに保存された情報資源へのアクセス制御に関するものである。
【背景技術】
【０００２】
従来、コンピュータに蓄積された情報資源を利用するに際し、情報資源と利用者とを対応付けて設定されたアクセス権限を登録したアクセスコントロールリストによりアクセス制限を行うことにより、セキュリティの向上を図っている。近年では、インターネットなどの広域ネットワークを介して、複数のネットワークを接続し、ファイルなどの資源を共有する分散環境を構築した超分散環境が普及しつつある。かかる環境においても、アクセスコントロールリストが使用されている。アクセスコントロールリストは、各ネットワークに存在するアクセス制御装置に管理されており、全てのネットワークのアクセス制御装置間で同期が取られている。
【０００３】
情報資源へのアクセス権限は、固定的なものではなく、種々の状況に応じて変化する。例えば、超分散環境において、特定のユーザの全アクセスを遮断しなければならない状況が発生した場合には、全てのアクセスコントロールリストに対して、アクセス権限を停止する旨の更新を同期的に行うことにより、特定のユーザのアクセスを遮断する、という技術が開示されている（特許文献１）。また、アクセス権限を認証する認証局により発行される証明書を、定期的に通知することにより、失効した証明書を持つユーザのアクセスを遮断する、という技術も開示されている（非特許文献１）。
【０００４】
【特許文献１】特開平１１－２８２８０５号公報
【非特許文献１】アイ・イー・ティー・エフ　アール・エフ・シー３２８０："インターネットX.509パブリックキー　インフラストラクチャー　サーティフィケイト　アンド　サーティフィケイト　リボケイション　リスト　（シー・アール・エフ）　プロファイル"（ＩＥＴＦ　ＲＦＣ３２８０："Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"）２００２年４月
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、例えば、解雇によるアクセス権限削除や、第３者による不正アクセスが発覚した場合など、緊急にアクセス遮断を実現しなければならない状況が発生した場合に、特許文献１記載の技術では、アクセスコントロールリストの更新に、非常に時間がかかり、緊急アクセス遮断を実現することは困難である場合がある。また、非特許文献１記載の技術においても、証明書の発行間隔、すなわち、証明書の更新間隔が定期的であり、発行間隔によっては、緊急アクセス遮断を実現することは困難であるという問題があった。
【０００６】
これらの課題は、超分散環境に特化した課題ではなく、複数のアクセス制御装置が連携してアクセス制御を行う場合の共通の課題であった。
【課題を解決するための手段】
【０００７】
上述の課題の少なくとも一部を解決するために、本発明は第１の構成として、以下の態様をとることとした。すなわち、ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、ネットワークには、ストレージ装置およびアクセス制御装置が複数接続されており、かかるアクセス制御装置は、各情報資源へのアクセス可否が登録されたアクセスコントロールリスト（以下「ＡＣＬ

」と呼ぶこととする）に基づき、アクセス可否の判断を行うアクセス判断部と、全ての情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限するアクセス制限部と、アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける情報入力部と、入力に基づき、ネットワークに接続された各アクセス制御装置がそれぞれ参照するアクセス禁止リストを更新する処理を行うリスト更新部とを備えることを要旨とする。

【０００８】

アクセス禁止ユーザを特定可能な情報とは、例えば、ユーザＩＤ、ユーザ名等が挙げられる。また、例えばＩＰアドレスなど、ユーザが利用している端末を特定する情報としてもよい。ＡＣＬには、例えば、読み取り専用、削除禁止、など詳細なアクセス権限の設定がされていることとしてもよいし、単に、アクセス許可、不許可が設定されていることとしても良い。

【０００９】

情報入力部は、例えば、ユーザから、キーボードなどの入力装置による直接入力を受け付けることとしてもよいし、アクセス禁止ユーザの登録されたファイルを読み込むことにより入力することとしてもよい。また、アクセス禁止リストそのものを取得することとしてもよい。リスト更新部は、例えば、アクセス禁止リストに登録されているユーザ情報を書き換えることにより更新することとしてもよいし、アクセス禁止リスト自体を差し替えることにより更新することとしてもよい。

【００１０】

このような構成をとることにより、複数のネットワークが、インターネットなどの広域ネットワークを介して接続されている超分散環境において、緊急アクセス遮断を行う必要のあるユーザ情報を、全てのネットワークのアクセス制御装置に通知することができ、緊急アクセス遮断を実現することができる。また、ＡＣＬは、情報資源ごとにアクセス許否が設定されているため、設定情報は膨大であり、更新処理に非常に時間がかかるが、アクセス禁止リストは、情報資源とは無関係にユーザ単位で全アクセスを禁止することとしており、データ量が軽いため、通知、更新処理の負荷を軽減することができる。

【００１１】

本発明のアクセス制御装置において、リスト更新部は、他のアクセス制御装置に対して、ユーザ情報を他のアクセス制御装置が参照する前記アクセス禁止リストに登録させる登録指示を配信することとしてもよい。こうすれば、ネットワークの負荷を軽減することができ、好適である。

【００１２】

本発明のアクセス制御装置において、リスト更新部は、更新されたアクセス禁止リストを、他のアクセス制御装置へ配信することとしてもよい。こうすれば、受信側のアクセス制御装置は、アクセス禁止リストを差し替えるだけで更新することができ、処理効率を向上することができる。

【００１３】

本発明の第２の構成として、ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、ネットワークには、ストレージ装置およびアクセス制御装置が複数接続されており、各情報資源のアクセス可否が登録されたＡＣＬに基づき、アクセス可否の判断を行うアクセス判断部と、ネットワークに接続された他のアクセス制御装置から、各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する受信部と、所定の情報により、アクセス禁止リストを更新するリスト更新部と、ＡＣＬよりアクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えることを要旨とする。

【００１４】

こうすれば、他のネットワークでアクセス禁止ユーザの登録要求が発生した場合にも、自ネットワークのアクセス制御装置に存在するアクセス禁止リストに、アクセス禁止ユーザを特定可能な所の情報を速やかに反映させることができる。従って、超分散環境におい

て、緊急アクセス遮断を効率的に実現することができる。

【００１５】

本発明の第１の構成および第２の構成におけるアクセス制御装置において、アクセス制限部は、未完了の処理を含めて、アクセス制限を行うこととしてもよい。こうすれば、アクセス禁止リスト更新後のアクセスのみでなく、アクセス禁止リスト更新前にアクセスされ開始された処理や、アクセス待ちの処理までも遮断することができ、利便性が向上する。

【００１６】

本発明の第１の構成および第２の構成におけるアクセス制御装置において、アクセス禁止リストに基づき、ＡＣＬを更新するＡＣＬ更新部を備えることとしてもよい。こうすれば、改めてＡＣＬを更新するための処理を行う必要がなく、利便性の向上を図ることができる。

【００１７】

本発明のアクセス制御装置において、前記ＡＣＬ更新後、前記アクセス禁止リスト内のユーザ情報を、所定のタイミングで削除する削除部を備えることとしてもよい。

【００１８】

例えば、アクセス禁止リストに一度登録されたユーザ情報が削除されないこととなると、アクセス禁止リストの内容が膨大となり、アクセス禁止リストの確認に時間を浪費する恐れがある。そのため、本発明のように、ACLの更新後に、アクセス禁止リストに登録されているユーザ情報を削除することとすれば、アクセス禁止リストの肥大を回避することができ、アクセス遮断処理の遅延を回避することが可能となる。また、アクセス禁止リスト自体を削除することとしても、本発明は実現可能である。

【００１９】

本発明のアクセス制御装置において、所定のタイミングとは、アクセス制御装置ごとに、ＡＣＬの更新の終了後としてもよい。こうすれば、各ネットワークに存在するアクセス制御装置は、個別に、ＡＣＬに更新済みのアクセス禁止ユーザ情報を削除することができる。アクセス制御装置は、ＡＣＬに先立ち、アクセス禁止リストを参照するため、本発明のように、ＡＣＬの更新終了を契機として、アクセス禁止リストに登録されているユーザ情報を削除することとすれば、アクセス制御装置の処理負荷を軽減することができる。

【００２０】

本発明のアクセス制限装置において、所定のタイミングとは、ネットワークに接続された全てのアクセス制御装置における、更新の終了後であることとしてもよい。

【００２１】

こうすれば、全てのアクセス制御装置で、ＡＣＬおよびアクセス禁止リストの同期を確保することができる。この方法は、例えば、アクセス禁止リスト自体が配信され、差し替えることによりアクセス禁止リストを更新する態様の場合に、有用性が高い。一部のアクセス制御装置においてＡＣＬの更新が終了していないにも関わらず、新しいアクセス禁止リストが配信されることによる既存のアクセス禁止リストの内容のＡＣＬへの反映漏れを回避することができる。本発明によれば、このような問題を回避しつつ、同期のとられたＡＣＬによって、アクセス遮断を行うことができる。

【００２２】

本発明は、また、第１の構成および第２の構成のアクセス制御装置を組合せ、第１の構成のアクセス制御装置は、自装置が参照する前記アクセス禁止リストに変更が発生した場合に、所定の情報、または、前記アクセス禁止リストを、前記ネットワークに接続された他のアクセス制御装置に配信する配信部を備え、第２の構成のアクセス制御装置は、所定の情報、または、アクセス禁止リストを受信し、自装置が参照するアクセス禁止リストを更新するリスト更新部を備えるアクセス制御システムとして構成することとしてもよい。

【００２３】

所定の情報を通知することとすれば、ネットワークに負荷をかけることなく処理を実行でき、処理効率を向上することができる。また、アクセス禁止リストを通知することとす

れば、緊急アクセス遮断を要するユーザが複数発生した場合には一度に通知することができ、また、アクセス禁止リスト自体を差し替えることで更新処理を行うことができるため、受信側のアクセス制御装置の処理負荷を軽減することができる。

【００２４】

本発明のアクセス制御システムにおいて、配信部は、他のアクセス制御装置へ、アクセス禁止リストを更新するための更新情報を同報配信することとしてもよい。こうすれば、全てのアクセス制御装置に対してまとめて通知することができ、好適である。

【００２５】

本発明のアクセス制御システムにおいて、アクセス禁止リストを更新するための更新情報を最初に配信するアクセス制御装置の配信部は、アクセス禁止リストを更新するための更新情報を、予め設定された他のアクセス制御装置へ配信し、かかる更新情報を受信した他のアクセス制御装置の配信部は、更に、予め設定された他のアクセス制御装置へ配信することとしてもよい。こうすれば、ネットワークのホップ数などを考慮した配信を行うことができ、利便性が向上する。

【００２６】

本発明は上述したアクセス制御装置、アクセス制御システムのほかに、アクセス制御方法として構成することもできる。また、上述のアクセス制御装置を実現するコンピュータプログラム、およびそのプログラムを記録した記録媒体、そのプログラムを含み搬送波内に具現化されたデータ信号など種々の態様で実現することが可能である。各態様において、先に示した種々の付加的要素を適用することが可能である。

【００２７】

本発明をコンピュータプログラムまたはそのプログラムを記録した記録媒体等として構成する場合には、アクセス制御装置、アクセス制御装置を制御するプログラム全体として構成するものとしてもよいし、本発明の機能を果たす部分のみを構成するものとしてもよい。また、記録媒体としては、フレキシブルディスクやＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、パンチカード、バーコードなどの符号が印刷された印刷物、コンピュータの内部記憶装置（ＲＯＭやＲＡＭ等のメモリ）および外部記憶装置などコンピュータが読み取り可能な種々の記録媒体を利用できる。

【発明を実施するための最良の形態】

【００２８】

以下、本発明の実施の形態について、以下の項目に分けて説明する。

Ａ．実施例：
Ａ１．システム構成：
Ａ２．機能ブロック：
Ａ３．アクセス制御処理：
Ａ４．ブラックリスト配信処理：
Ａ５．アクセス遮断処理：
Ａ６．ＡＣＬ更新処理：
Ｂ．変形例：

【００２９】

Ａ．実施例：

Ａ１．システム構成：

図１は、本発明の実施例におけるシステム構成を例示する説明図である。アクセス制御システム１０００は、インターネットＩＮＴを介して、４つのネットワークＡ，Ｂ，Ｃ，Ｄから構成されている。ネットワークＡは、アクセス制御装置１００、ストレージ５００、クライアントＣＬ１等が、ローカルエリアネットワークＬＡＮ１を介して接続されている。ネットワークＢ，Ｃ，Ｄも同様に、アクセス制御装置２００，３００，４００と、ストレージ６００，７００，８００と、クライアントＣＬ２，ＣＬ３、ＣＬ４とが、それぞれ、ローカルエリアネットワークＬＡＮ２，ＬＡＮ３，ＬＡＮ４を介して接続されている。

【００３０】
各ストレージには、データファイル５０１，６０１，７０１，８０１等が格納されており、アクセス制御システム１０００は、インターネットＩＮＴを介した、いわゆる、超分散環境を構築している。各クライアントは、自己が接続されているネットワークのストレージ装置のみでなく、他のネットワークに接続されたストレージ装置内に格納されているデータファイルを参照することができる。すなわち、クライアントＣＬ１は、ストレージ５００内のデータファイル５０１にアクセスすることができるだけでなく、ネットワークＣに存在するストレージ７００内のデータファイル７０１にアクセスすることもできる。
【００３１】
各ストレージ内のデータファイルにアクセスするためには、アクセス権限の許否が判断される。かかるアクセス権限の許否の判断は、アクセス制御装置が行う。クライアントＣＬ１がデータファイル５０１にアクセス要求を行うと、アクセス制御装置１００は、クライアントＣＬ１のユーザの、データファイル５０１へのアクセス権限の許否確認を要求し、かかる確認結果に基づき、データファイルへのアクセスを制御する。
【００３２】
アクセス制御装置１００は、データファイルなどのオブジェクトのアクセス権限がユーザごとに詳細に設定されたアクセスコントロールリスト１１０（以降、ＡＣＬ１１０と呼ぶこととする）と、ＡＣＬ１１０に登録されておらず、緊急に全てのアクセスを禁止する必要のあるユーザ情報が登録されたアクセス禁止リスト１２０（以降、「ブラックリスト１２０」と呼ぶこととする）とを管理している。アクセス制御装置１００は、アクセス要求を受け付けると、まず、アクセス要求を行ったユーザのユーザ情報がブラックリスト１２０に登録されているか否かを判断し、登録されていない場合には、ＡＣＬ１１０を参照してアクセス許否を判断する。
【００３３】
アクセス制御装置１００は、ネットワークＡで、例えば解雇によるアクセス権限削除など、緊急にアクセスを遮断する必要のあるユーザが発生した場合に、管理者の操作に応じて、自己のブラックリスト１２０を更新し、他のアクセス制御装置２００，３００，４００に対して、かかるユーザ情報を、それぞれのブラックリスト２２０，３２０，４２０へ登録させる指示を配信する。アクセス制御装置２００，３００，４００は、かかる登録指示を受信して、自己のブラックリスト２２０，３２０，４２０を更新する。こうすることによって、超分散環境において、緊急アクセス遮断を必要とするユーザが発生した場合にも、全てのネットワークで、効率的に緊急アクセス遮断を行うことができる。
【００３４】
Ａ２．機能ブロック：
図２は、アクセス制御装置１００の機能ブロックを例示する説明図である。アクセス制御装置１００は、主制御部１０１と、通信部１０２と、ＡＣＬ管理部１０３と、ブラックリスト管理部１０４と、アクセス制御部１０５と、アクセス制御部１０５の一部として構成されているアクセス制限部１０６と、アクセス遮断部１０７と、入力部１０８と、ストレージ管理部１０９とから構成されている。通信部１０２は、アクセス制御装置１００が接続されているローカルエリアネットワークＬＡＮ１内の他の器機との通信、インターネットＩＮＴを介した他のネットワークとの通信等を制御する。
【００３５】
ＡＣＬ管理部１０３は、オブジェクト毎に、ユーザの詳細なアクセス権限を登録したＡＣＬ１１０を管理しており、ＡＣＬ１１０の更新等を行う。ＡＣＬ１１０の詳細は後述する。ブラックリスト管理部１０４は、解雇など、緊急にアクセスを遮断する必要のあるユーザが発生した場合、かかるユーザのユーザＩＤとユーザ名が登録されるブラックリスト１２０を管理する。登録されるユーザＩＤおよびユーザ名は、管理者により、入力部１０８を介して入力される。ブラックリスト１２０の内容は後述する。ＡＣＬ管理部１０３は、また、情報の授受を行いながら、ブラックリスト１２０に登録されているユーザ情報により、ＡＣＬ１１０を更新する機能を奏する。アクセス制御装置１００は、本来ＡＣＬの

みによりアクセス制御を行うことが処理効率の観点からも好ましいため、ブラックリスト１２０に登録されたアクセス遮断が必要なユーザ情報に基づき、ＡＣＬ１１０から遮断対象ユーザに関する情報を削除する。

【００３６】

ストレージ管理部１０９は、アクセス制御装置１００と同一ネットワーク、すなわち、ローカルエリアネットワークＬＡＮ１に接続されているストレージ５００等のストレージ装置を管理する。具体的には、各ストレージに格納されているデータ情報や、各ストレージ装置にアクセスしているユーザ等を管理している。図にアクセスの状態を表したアクセス管理表１０９ａを併せて示した。

【００３７】

アクセス管理表１０９ａは、各アクセスに固有に割り振られたアクセスＩＤと、オブジェクト名称と、アクセス状態と、アクセスユーザとから構成されている。例えば、ジョブＩＤ「１」のオブジェクト「Ｏ－９」は、「アクセス中」であり、アクセスしているユーザは「Ｓ－３」であることを示している。同様に、アクセスＩＤ「２」のオブジェクト「Ｏ－７」は、「アクセス待ち」であり、ユーザは「Ｓ－８」であることを示している。

【００３８】

アクセス制御部１０５は、ＡＣＬ１１０によるアクセス制限や、緊急アクセス遮断などアクセスに関する処理を制御する機能を奏する。アクセス制限部１０６は、アクセス制御部１０５の一部として構成されており、ユーザのアクセス権限の確認要求を受け付けると、ＡＣＬ１１０を参照して、結果をストレージ５００に通知する。アクセス遮断部１０７は、同じく、アクセス制御部１０５の一部として構成されており、ブラックリスト１２０、および、アクセス管理表１０９ａを参照して、アクセス管理表１０９ａに存在するユーザが、ブラックリスト１２０に登録されているユーザ、すなわち、緊急にアクセスを遮断しなければならないユーザである場合には、アクセス中、アクセス待ちに関わらず、即座に遮断する機能を奏する。例えば、ユーザＩＤ「Ｓ－１」のユーザが、ブラックリスト１２０に登録されている場合には、アクセスＩＤ「３」および「６」のアクセスが遮断されることとなる。

【００３９】

図３（ａ）は、本実施例におけるＡＣＬを例示する説明図である。ＡＣＬ１１０は、設定されたアクセス権限に固有に割り振られた「ＩＤ」と、オブジェクト名を示す「オブジェクト」と、管理ユーザ名を示す「ユーザ」と、アクセス可能なグループを表す「グループ」と、アクセス権限を示す「アクセス」とから構成される。グループを図３（ｂ）に示した。破線で示されるグループ「Ｇ－１」には、ユーザＩＤが「Ｓ－１」、「Ｓ－２」、「Ｓ－３」、「Ｓ－４」、「Ｓ－５」というユーザが含まれる。更に、一点鎖線に示すようにグループ「Ｇ－２」は、「Ｇ－１」の一部であり、ユーザ「Ｓ－１」、「Ｓ－２」、「Ｓ－５」が含まれる。ユーザ「Ｓ－１」、「Ｓ－２」、「Ｓ－５」は、グループ「Ｇ－１」および「Ｇ－２」の双方に属することとなる。

【００４０】

アクセス権限は、図３（ａ）の右下に示すように、「Ｒ」は「Ｒｅａｄ」すなわち「読み取り可能」を表しており、「Ｗ」は「Ｗｒｉｔｅ」すなわち「書き込み可能」を表している。例えば、ＩＤ「１」のオブジェクト「Ｏ－１」は、ユーザ「Ｓ－３」により「Ｒ，Ｗ」すなわち、読み取り、書き込みが可能であることを示している。また、ＩＤ「２」に示すように、オブジェクト「Ｏ－１」は、更に、グループ「Ｇ－１」に属するユーザに、「Ｒ」すなわち「読み取り可能」というアクセスを認めていることとなる。

【００４１】

図４は、本実施例におけるブラックリスト１２０の内容を例示する説明図である。ブラックリスト１２０は、ユーザＩＤと、ユーザ名とから構成される。ユーザＩＤ、ユーザ名のいずれかのみから構成されることとしてもよい。本実施例では、アクセス制御装置１００でアクセス遮断要求を受け付け、ユーザＩＤ「Ｓ－１」、ユーザ名「Ｔａｒｏ　Ｈｉｔａｃｈｉ」というユーザのアクセスを遮断すべくブラックリスト１２０に登録した状態を

示した。本実施例では、かかるユーザのみしかブラックリスト１２０に登録されていないが、一度に複数のユーザを登録することも可能である。また、既にブラックリストに登録されており、新たに、アクセス遮断すべきユーザを追加することも可能である。

【００４２】

他のアクセス制御装置２００，３００，４００も同様の構成であるため、説明は省略する。

【００４３】

Ａ３．アクセス制御処理：

図５は、本実施例におけるアクセス制御処理を説明するチャート図である。クライアントＣＬ１が、ストレージ５００内のデータファイル５０１にアクセスを要求する場合の処理を表している。

【００４４】

クライアントＣＬ１は、アクセス制御装置１００にアクセス要求を送出する（ステップＳａ１００）。アクセス制御装置１００は、かかる要求を受け付け、アクセス権限の確認要求を行い、ブラックリスト１２０およびＡＣＬ１１０に基づき、アクセス許否を判断する（ステップＳａ１０１）。アクセス制御装置１００は、かかる結果に基づき、ストレージ５００にアクセスを行い（ステップＳａ１０２）、アクセス結果を、自己を介して（ステップＳａ１０３）、クライアントＣＬ１へ通知する（ステップＳａ１０４）。

【００４５】

図６は、アクセス制御処理を説明するフローチャートである。アクセス制御装置１００が行う処理であり、図５のステップＳａ１０１に相当する処理である。

【００４６】

アクセス制御装置１００は、クライアントＣＬ１からストレージ５００へのアクセス権限の確認要求を、ユーザＩＤ、アクセス対象オブジェクト名とともに受信する（ステップＳ１０）と、ブラックリスト１２０を参照し（ステップＳ１１）、かかるユーザがブラックリスト１２０に登録されているか否かを判断する（ステップＳ１２）。ブラックリスト１２０に登録されている場合には、アクセス遮断対象ユーザであるため、ストレージ５００に対して、アクセス不許可通知を送出する（ステップＳ１６）。

【００４７】

かかるユーザがブラックリスト１２０に登録されていない場合には、ＡＣＬ１１０を参照し、アクセス対象オブジェクトのアクセス許否の詳細を確認する（ステップＳ１３）。アクセス制御装置１００は、アクセス許否を判断し（ステップＳ１４）、アクセスが許可されている場合（ステップＳ１４：ＹＥＳ）には、読み取り可能、書き込み可能などのアクセス制限内容に基づき、ストレージ５００にアクセスする（ステップＳ１５）。ブラックリスト１２０には登録されていない（ステップＳ１２：ＮＯ）が、ＡＣＬ１１０において、アクセスが許可されていない場合（ステップＳ１４：ＮＯ）には、クライアントＣＬ１に対してアクセス不許可通知を送出する（ステップＳ１６）。

【００４８】

Ａ４．ブラックリスト配信処理：

図７は、本実施例におけるブラックリスト配信処理を説明するフローチャートである。アクセス制御装置１００は、アクセス遮断要求を管理者から受け付けると、自己のブラックリスト１２０に、アクセス遮断対象ユーザのユーザ情報を登録するとともに、かかるユーザ情報の登録指示を、アクセス制御装置２００、３００，４００に対して一度に送出する。図７では、説明の便宜上、アクセス制御装置１００からアクセス制御装置２００に登録指示が送出される処理を示した。

【００４９】

アクセス制御装置１００は、アクセス遮断要求を管理者から受け付ける（ステップＳ２０）と、アクセス遮断を行うユーザのユーザＩＤとユーザ名をブラックリスト１２０へ登録する（ステップＳ２１）。そして、他のネットワークに接続されたアクセス制御装置２００，３００，４００に対して、かかるアクセス遮断対象ユーザを各アクセス制御装置内

のブラックリストへ登録するよう、ユーザＩＤおよびユーザ名と併せて登録指示を送出する（ステップＳ２２）。

【００５０】

次に、アクセス制御装置１００は、ブラックリストに登録されたユーザが、ストレージ５００内のオブジェクトに、アクセス中、もしくはアクセス待ちの状態である場合、かかるアクセスを即座に遮断する（ステップＳ２３）。そして、ブラックリストに基づき、ＡＣＬを更新し（ステップＳ２４）、更新終了後、ブラックリスト１２０からユーザ情報を削除する（ステップＳ２５）。

【００５１】

アクセス制御装置２００は、ステップＳ２２において送出された登録指示を受信する（ステップＳ３０）と、ブラックリストにユーザＩＤとユーザ名を追加し、ブラックリスト２２０を更新する（ステップＳ３１）。ブラックリスト２２０の更新を終えると、アクセス遮断すべきユーザのアクセスを遮断し（ステップＳ３２）、ＡＣＬを更新して（ステップＳ３３）、ブラックリスト２２０からユーザ情報を削除する（ステップＳ３４）。ステップＳ３２～ステップＳ３４までの処理は、アクセス制御装置１００におけるステップＳ２３～ステップＳ２５と同様である。アクセス遮断処理（ステップＳ２３、ステップＳ３２）およびＡＣＬ更新処理（ステップＳ２４、ステップＳ３３）については後述する。

【００５２】

Ａ５．アクセス遮断処理：

図８は、本実施例におけるアクセス遮断処理を説明するフローチャートである。アクセス制御装置１００のアクセス遮断部１０７が実行する処理であり、図７のステップＳ２３に相当する処理である。図７のステップＳ３２において、アクセス制御装置２００が実行する処理も同様である。

【００５３】

アクセス制御装置１００は、ブラックリスト１２０およびアクセス管理表１０９ａを参照し（ステップＳ４０、Ｓ４１）、ブラックリスト１２０に登録されているユーザが、ストレージ５００内のオブジェクトにアクセス中、もしくは、アクセス待ちの状態であるか否か判断する（ステップＳ４２）。アクセス中、もしくは、アクセス待ちである場合には、かかるユーザのアクセスを、アクセス中、アクセス待ちにかかわらず、すべて遮断する（ステップＳ４３）。アクセス中、もしくは、アクセス待ちオブジェクトが存在しない場合には、処理を終了する。

【００５４】

Ａ６．ＡＣＬ更新：

図９は、本実施例におけるＡＣＬを更新する処理を説明するフローチャートである。図７のステップＳ２４に相当する処理である。図７のステップＳ３３において、アクセス制御装置２００が実行する処理も同様である。本実施例では、ユーザＩＤ「Ｓ－１」、ユーザ名「Ｔａｒｏ　Ｈｉｔａｃｈｉ」というユーザを、アクセス遮断対象ユーザとした。

【００５５】

アクセス制御装置１００は、ブラックリスト１２０およびＡＣＬ１１０を参照し（ステップＳ５０）、グループ情報から、ユーザＩＤ「Ｓ－１」を削除する（ステップＳ５１）。次に、アクセス制御装置１００は、ＡＣＬ１１０から、ユーザＩＤが「Ｓ－１」であるＩＤを抽出し削除する（ステップＳ５１）。本実施例では、図に太矢印で示すように、ＩＤ「５」が削除される。

【００５６】

こうすれば、グループに関する情報を維持しつつ、ユーザＩＤ「Ｓ－１」が関係するＡＣＬ１１０を更新することができる。

【００５７】

以上説明した実施例によれば、超分散環境において、あるユーザのアクセス権限を、緊急に停止したい状況が発生した場合に、かかるユーザの情報を全てのネットワークのアクセス制御装置に、速やかに通知することができる。また、図９で説明したように、ＡＣＬ

を更新するには、多くの工数がかかるため、本発明のようにブラックリストを配置し、ＡＣＬより先にブラックリストを参照してアクセス遮断を行うことにより、セキュリティの向上を図ることができる。

【００５８】

Ｂ．変形例：

以上、本発明の種々の実施例について説明したが、本発明はこれらの実施例に限定されることなくその趣旨を逸脱しない範囲内で種々の構成を取ることができることはいうまでもない。例えば、以下のような変形が可能である。

【００５９】

Ｂ１．変形例１：

上述した実施例では、アクセス制御装置１００から他のアクセス制御装置２００，３００，４００へ、アクセス遮断対象ユーザのユーザ情報を、各アクセス制御装置のブラックリストに登録させる登録指示を送出することとしたがこれに限られない。例えば、アクセス制御装置１００で更新したブラックリストの複製を他のアクセス制御装置２００，３００，４００へ配布することとしてもよい。こうすれば、ブラックリスト受信側のアクセス制御装置は、ブラックリストを差し替えるだけで更新することができ、処理効率を向上することができる。

【００６０】

また、上述した実施例では、ＡＣＬ更新後、ブラックリストに登録されているユーザ情報を削除することとしたが、本変形例のように、ブラックリストを配布する場合には、ブラックリストそのものを削除することとしてもよい。図１０に、本変形例におけるブラックリスト削除処理を説明するフローチャートを示した。本変形例では、アクセス制御装置１００は、ＡＣＬの更新を終了しているものとする。

【００６１】

アクセス制御装置２００は、ＡＣＬの更新を終了する（ステップＳａ２００）と、ブラックリスト配布元のアクセス制御装置１００へ、更新終了通知を送出する（ステップＳａ２０１）。同様に、アクセス制御装置４００およびアクセス制御装置３００も、ＡＣＬの更新を終了すると、更新終了通知を送出する（ステップＳａ２０２～ステップＳａ２０５）。

【００６２】

アクセス制御装置１００は、他のアクセス制御装置の全てから更新終了通知を受信すると、自己のブラックリストを削除する（Ｓａ２０７）と共に、他のアクセス制御装置にブラックリストの削除指示を送出し、かかる削除指示を受信した他のアクセス制御装置２００，３００，４００は、ブラックリストを削除する（ステップＳａ２０８～Ｓａ２１４）。

【００６３】

このような構成をとることにより、全てのアクセス制御装置において、ＡＣＬの同期を取ることができる。例えば、連続して緊急アクセス遮断要求が発生し、短時間に複数回ブラックリストの配布が行われるような場合には、ＡＣＬにユーザ情報が未反映の状態のブラックリストが、後続のブラックリストによって更新されることを回避することができる。

【００６４】

Ｂ２．変形例２：

上述の実施例では、アクセス制御装置１００から他のアクセス制御装置２００，３００，４００へ、同時にブラックリストを配布することとしたが、これに限られない。例えば、図１１に示すように、各アクセス制御装置は、ブラックリストを、予め設定された他のアクセス制御装置へ逐次的に配信することとしてもよい。図に太線矢印で示すように、アクセス制御装置１００は、ブラックリストをアクセス制御装置２００へ配信し、アクセス制御装置２００はアクセス制御装置３００に配信し、アクセス制御装置３００は、アクセス制御装置４００へ配信する。こうすれば、ネットワークのホップ数などを考慮した配信

を行うことができ、利便性が向上する。

【００６５】

Ｂ３．変形例３：

また、例えば、上述した実施例の超分散環境に、更に、ユーザが正規のユーザであることを証明する証明書を管理する認証局を設置することとしてもよい。かかる場合には、認証局において、証明書の認証に先立ち、ブラックリストによるアクセス制御を行うこととすれば、セキュリティを向上することができ、好適である。

【図面の簡単な説明】

【００６６】

【図１】本実施例におけるシステム構成図である。

【図２】本実施例におけるアクセス制御装置の機能ブロック図である。

【図３】本実施例におけるアクセスコントロールリストを例示する説明図である。

【図４】本実施例におけるブラックリストを例示する説明図である。

【図５】本実施例におけるアクセス制御処理を説明するチャート図である。

【図６】本実施例におけるアクセス制御処理を説明するフローチャートである。

【図７】本実施例におけるアクセス権限確認処理を説明するフローチャートである。

【図８】本実施例におけるアクセス遮断処理を説明するフローチャートである。

【図９】本実施例におけるＡＣＬ更新処理を説明するフローチャートである。

【図１０】変形例におけるブラックリスト削除処理を説明するフローチャートである。

【図１１】変形例におけるシステム構成図である。

【符号の説明】

【００６７】

１０００...アクセス制御システム

１００，２００，３００，４００...アクセス制御装置

１１０，２１０，３１０，４１０...ＡＣＬ

１２０，２２０，３２０，４２０...ブラックリスト

５００，６００，７００，８００...ストレージ

５０１，６０１，７０１，８０１...データファイル

１０１...主制御部

１０２...通信部

１０３...ＡＣＬ管理部

１０４...ブラックリスト管理部

１０５...アクセス制御部

１０６...アクセス制限部

１０７...アクセス遮断部

１０８...入力部

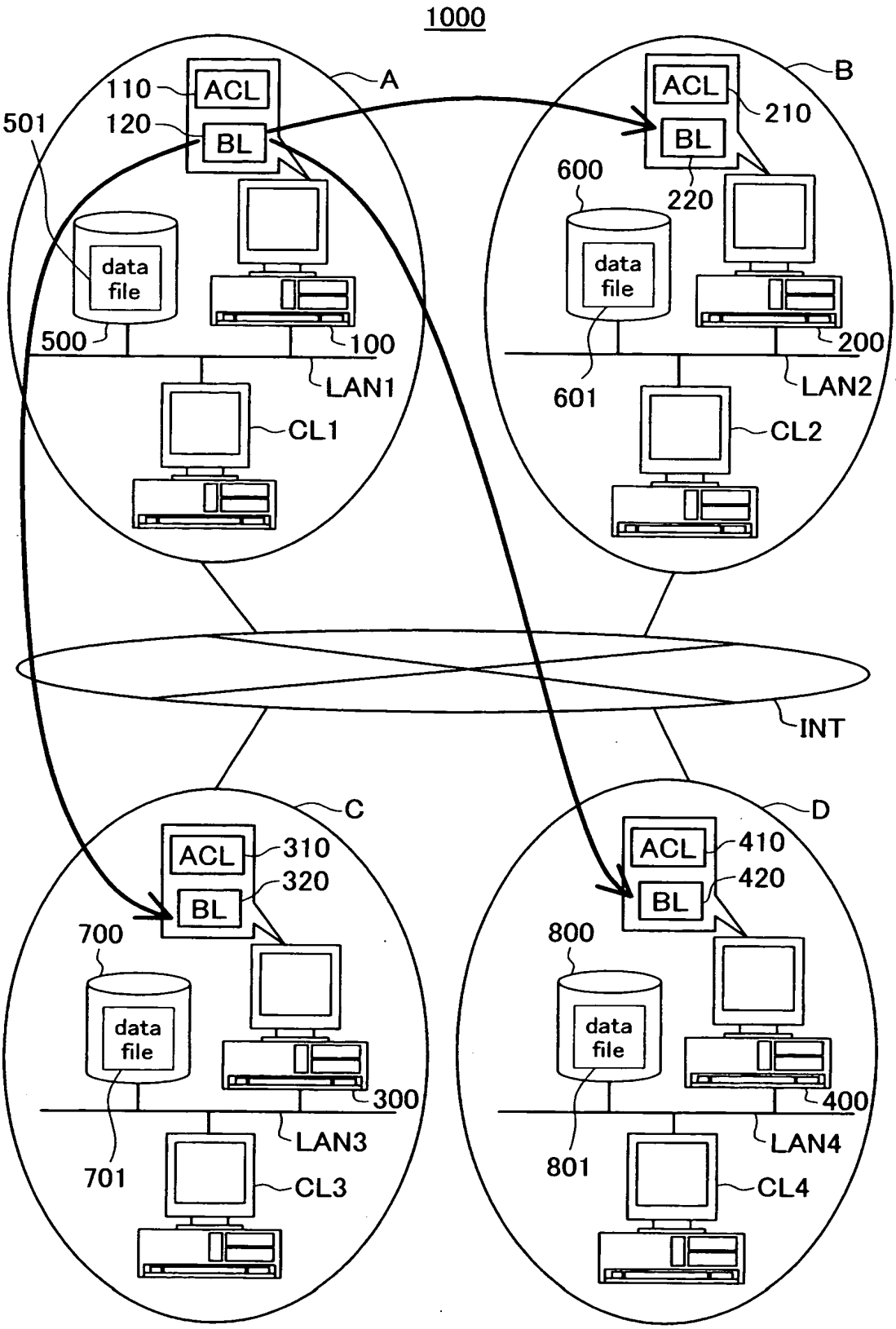
１０９...ストレージ管理部

１０９ａ...アクセス管理表

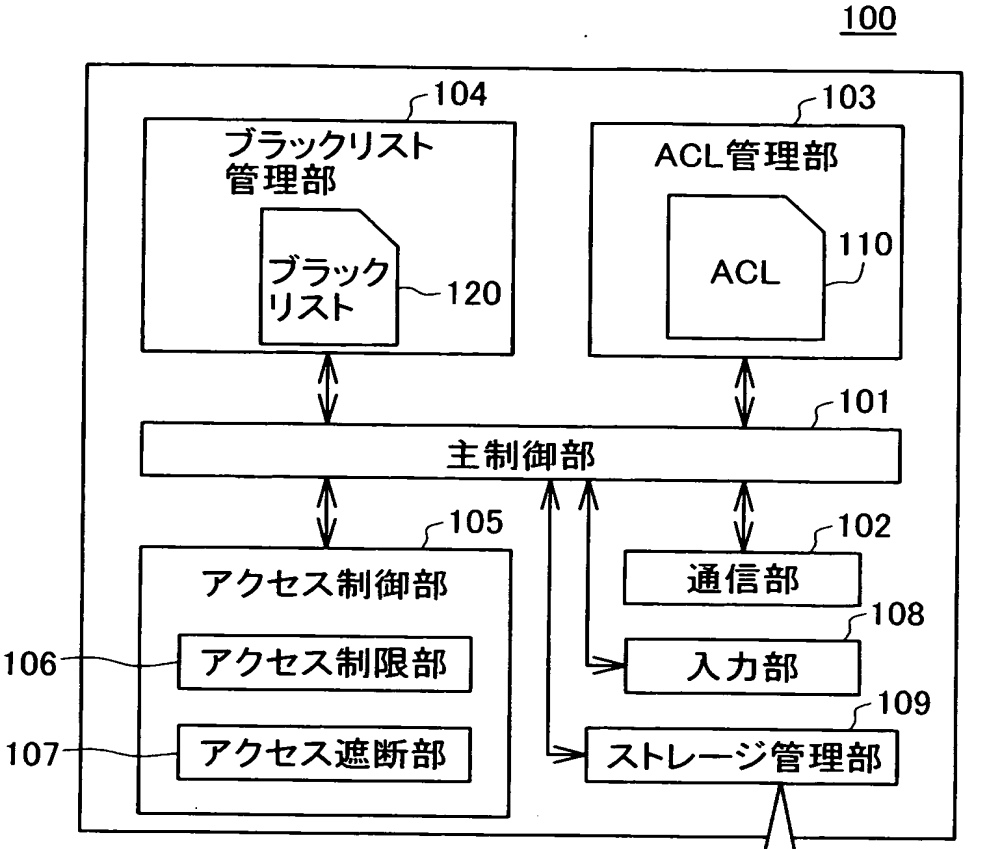
１１０...アクセスコントロールリスト

１２０...ブラックリスト

【書類名】図面
【図１】


1000
A
B
C
D
110
ACL
120
BL
501
data file
500
100
LAN1
CL1
210
220
600
200
601
LAN2
CL2
INT
310
320
700
300
701
LAN3
CL3
410
420
800
400
801
LAN4
CL4

【図２】



109a

ID	オブジェクト	状態	ユーザ
1	O－9	アクセス中	S-3
2	O－7	アクセス待ち	S-8
3	O－1	アクセス中	S-1
4	O－6	アクセス中	S-5
5	O－4	アクセス中	S-8
6	O－5	アクセス待ち	S-1

【図３】

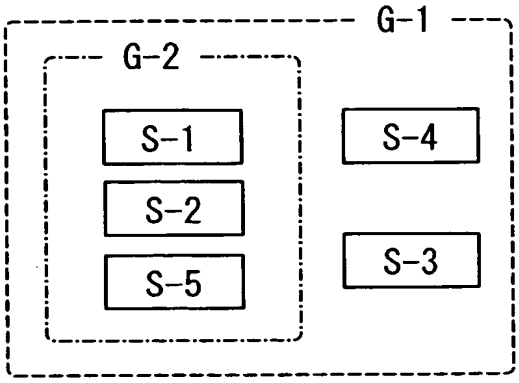
(a)

110

ID	オブジェクト	ユーザ	グループ	アクセス
1	O-1	S-3	—	R, W
2	O-1	—	G-1	R
3	O-2	S-7	—	R, W
4	O-2	—	G-2	R
5	O-3	S-1	—	R, W
6	O-3	—	G-2	R

R-Read
W-Write

(b)

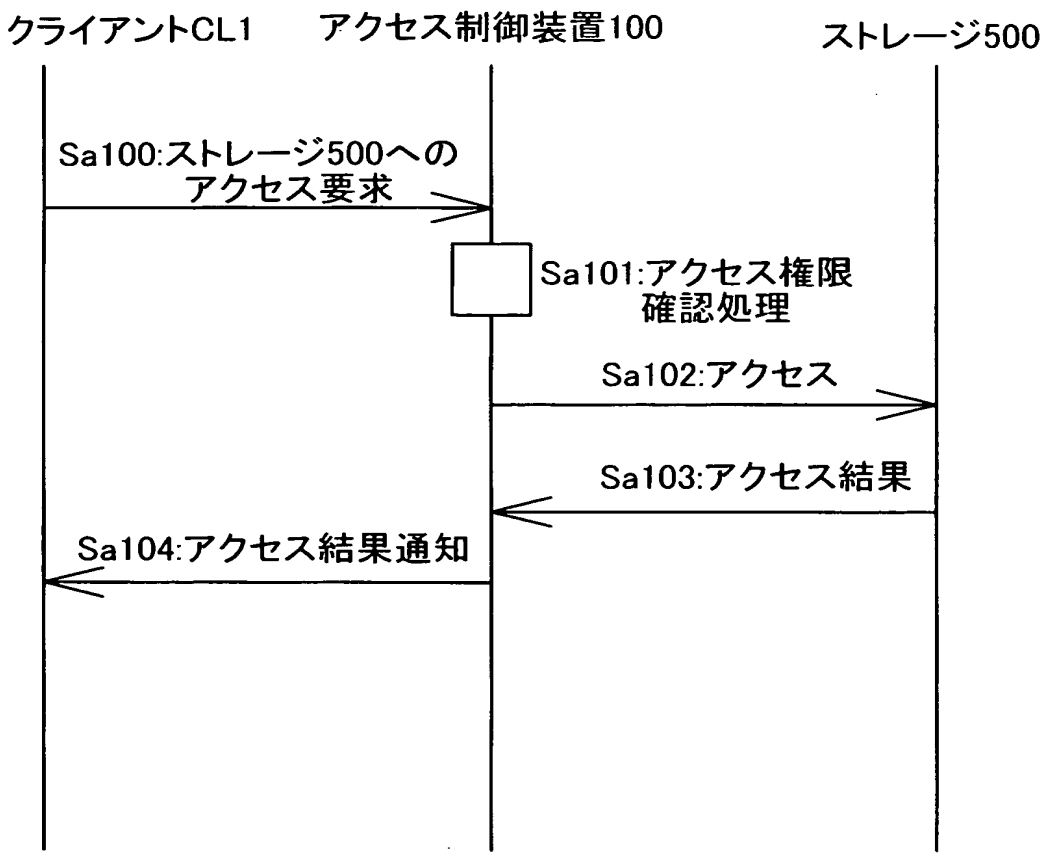


【図４】

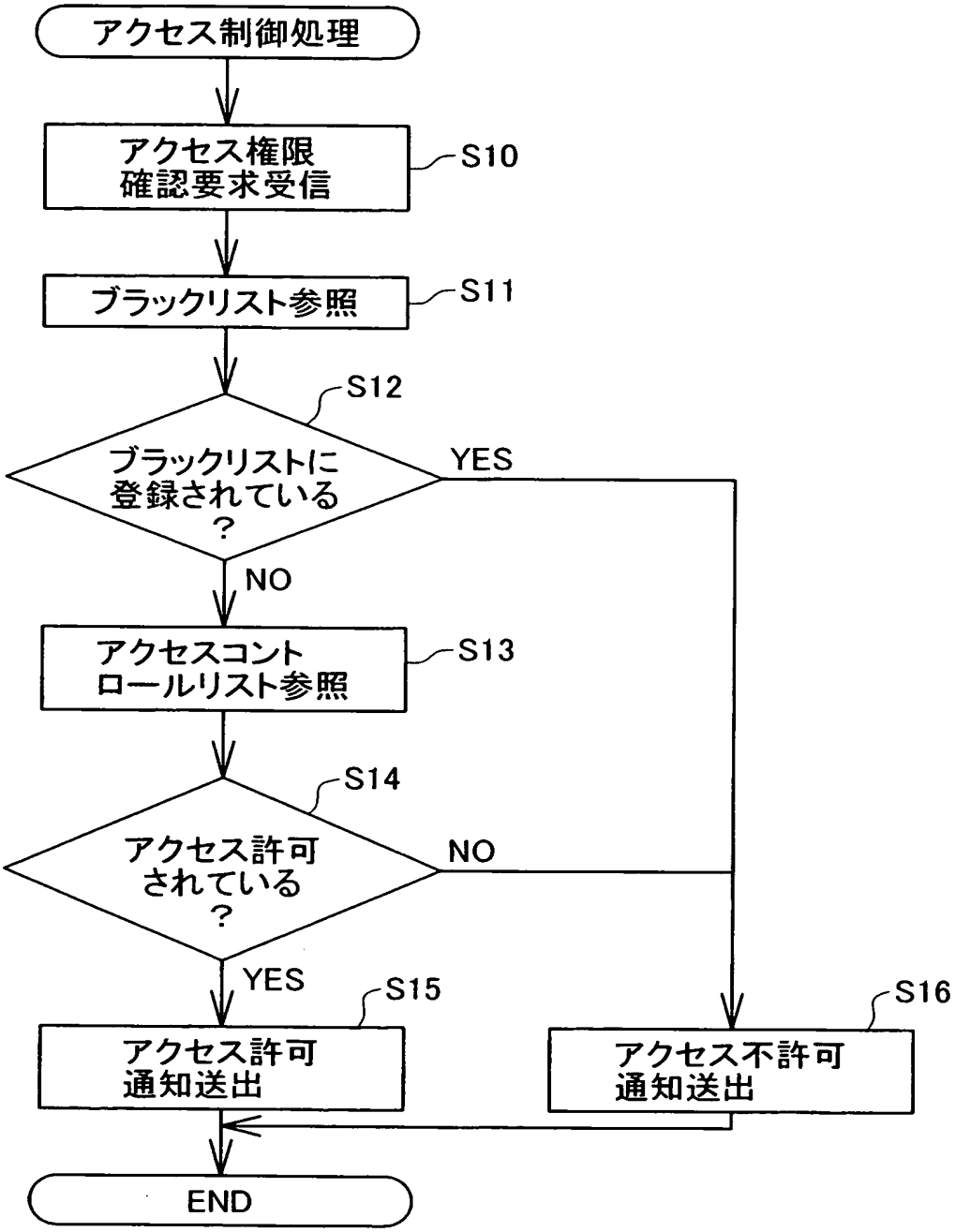
120

User ID	User Name
S-1	Taro Hitachi

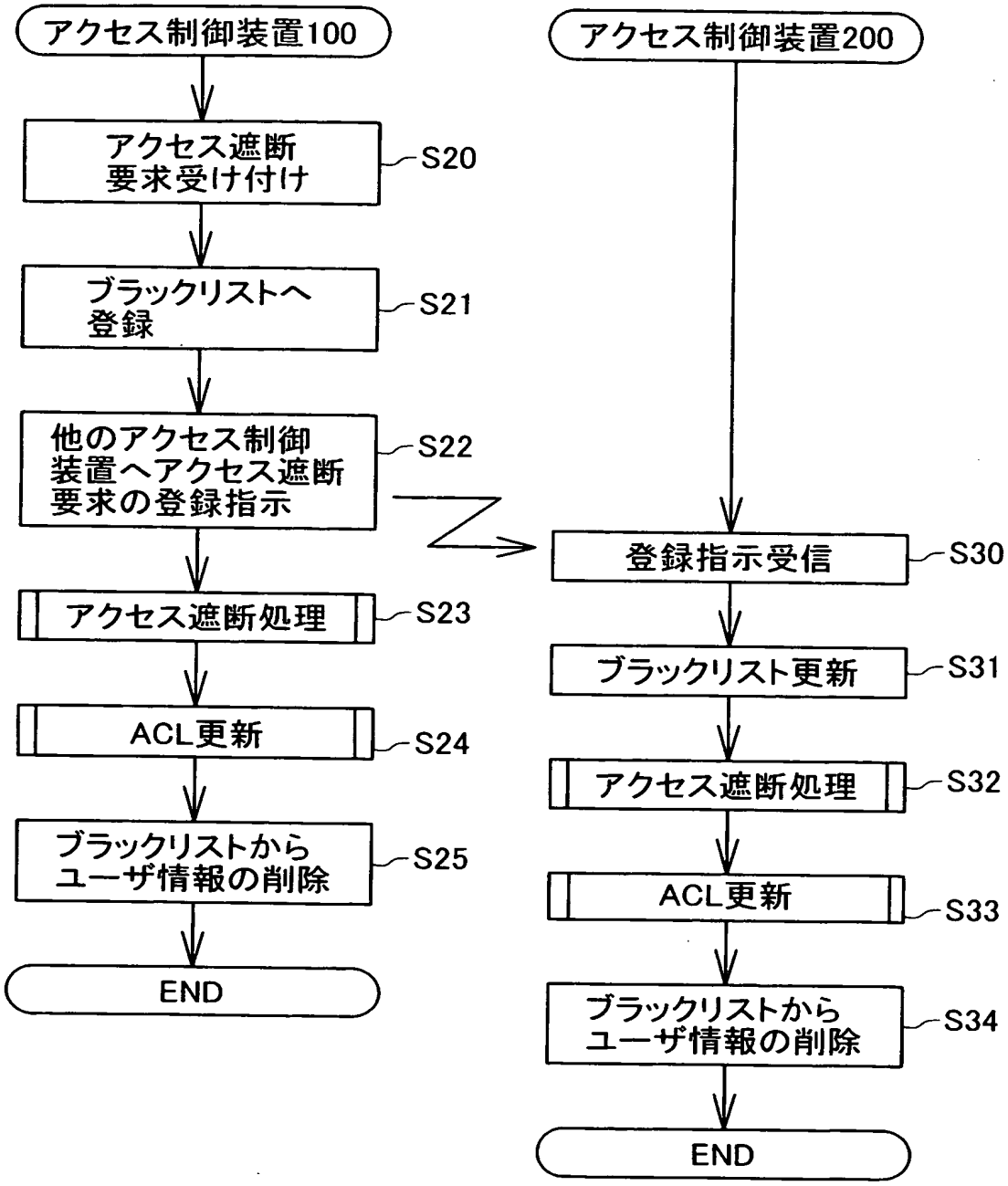
【図５】


クライアントCL1
アクセス制御装置100
ストレージ500
Sa100:ストレージ500へのアクセス要求
Sa101:アクセス権限確認処理
Sa102:アクセス
Sa103:アクセス結果
Sa104:アクセス結果通知

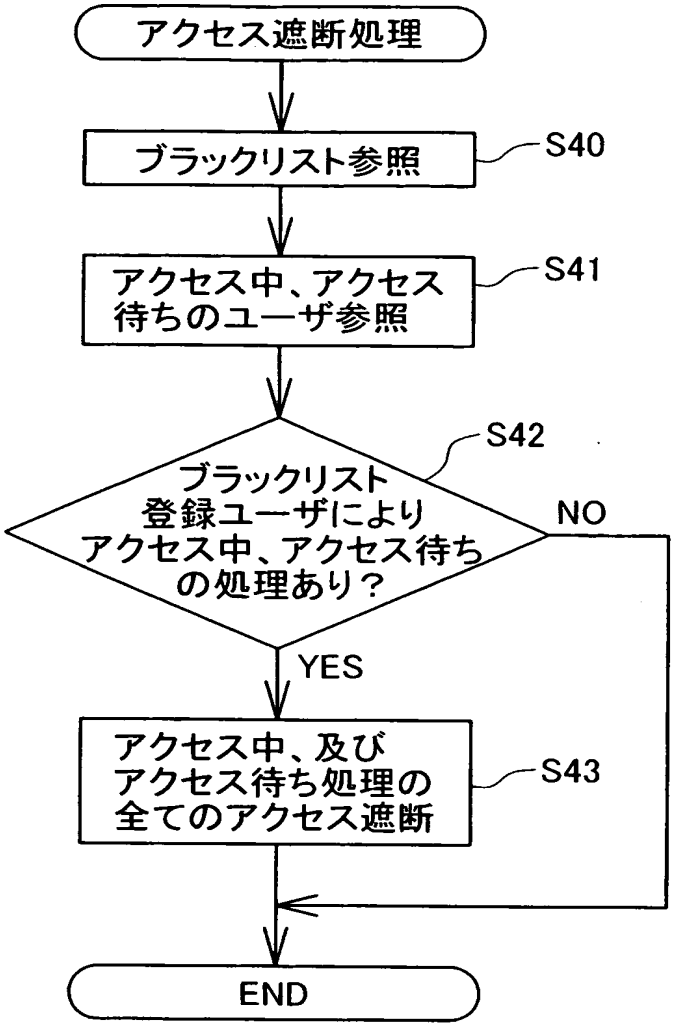
【図６】


アクセス制御処理
アクセス権限
確認要求受信
S10
ブラックリスト参照
S11
S12
ブラックリストに
登録されている
？
YES
NO
アクセスコント
ロールリスト参照
S13
S14
アクセス許可
されている
？
NO
YES
S15
アクセス許可
通知送出
S16
アクセス不許可
通知送出
END

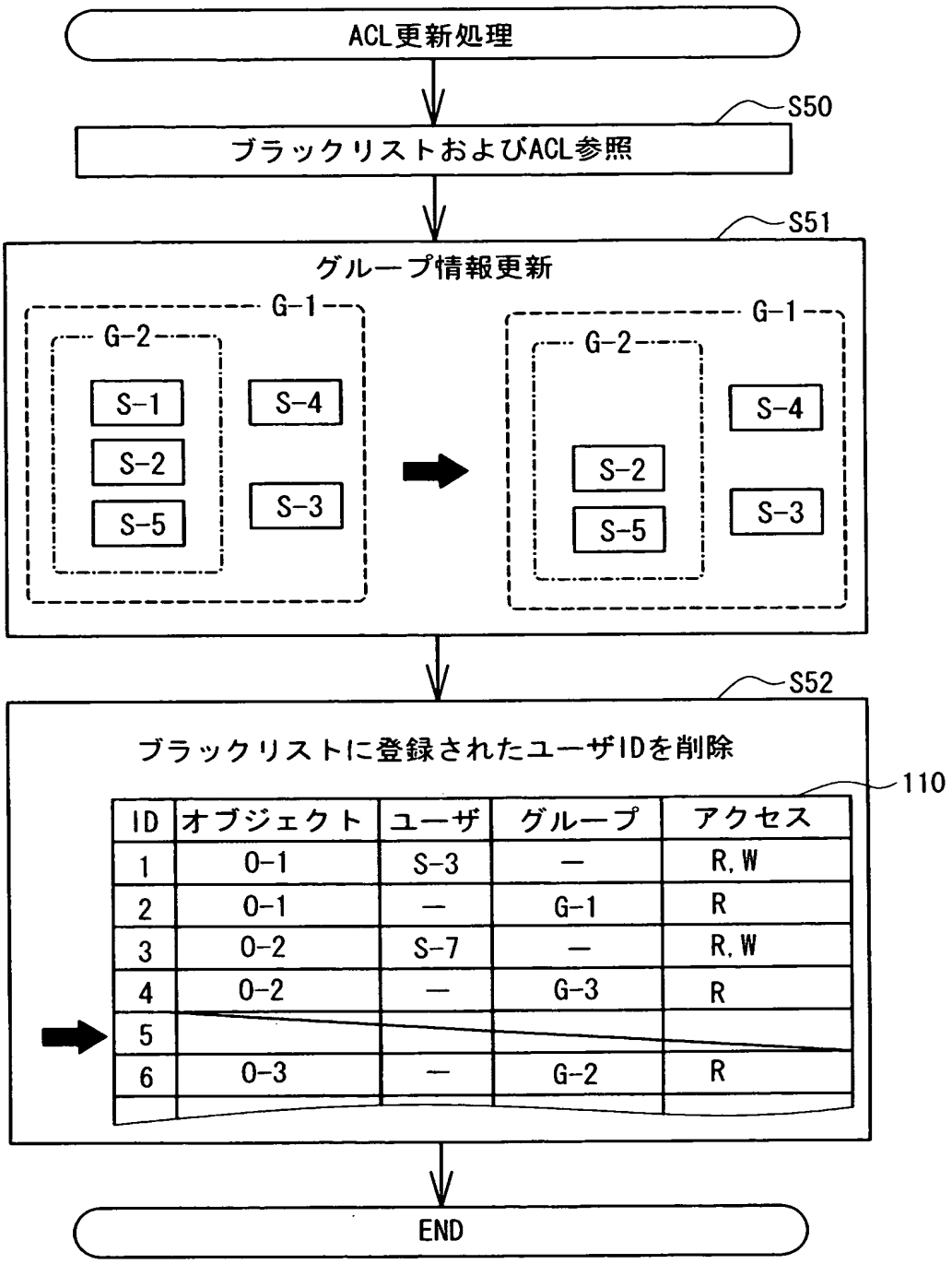
【図７】


アクセス制御装置100
アクセス遮断
要求受け付け
S20
ブラックリストへ
登録
S21
他のアクセス制御
装置へアクセス遮断
要求の登録指示
S22
アクセス遮断処理
S23
ACL更新
S24
ブラックリストから
ユーザ情報の削除
S25
END
アクセス制御装置200
登録指示受信
S30
ブラックリスト更新
S31
アクセス遮断処理
S32
ACL更新
S33
ブラックリストから
ユーザ情報の削除
S34
END

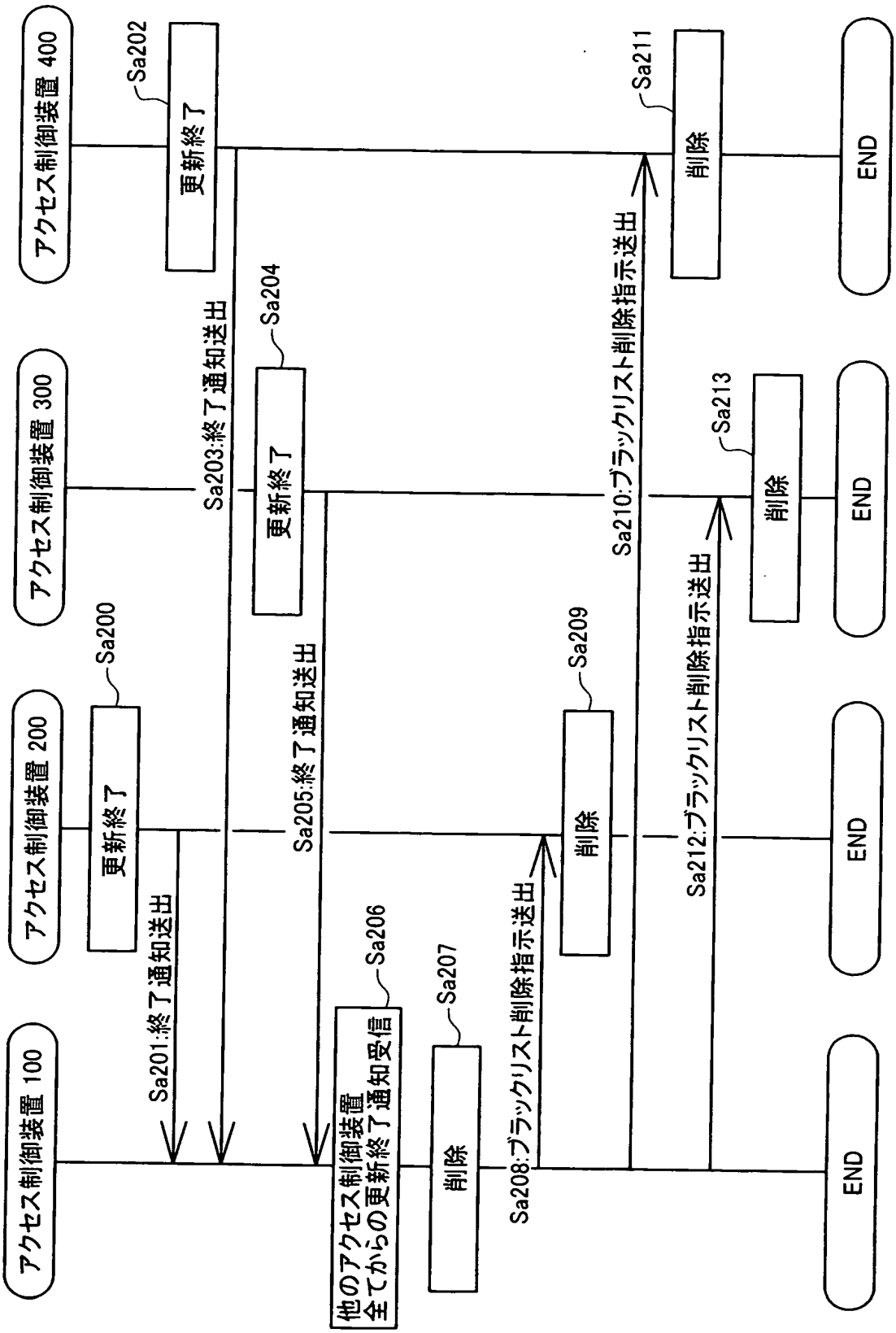
【図８】


アクセス遮断処理
ブラックリスト参照
S40
アクセス中、アクセス待ちのユーザ参照
S41
S42
ブラックリスト登録ユーザによりアクセス中、アクセス待ちの処理あり？
NO
YES
アクセス中、及びアクセス待ち処理の全てのアクセス遮断
S43
END

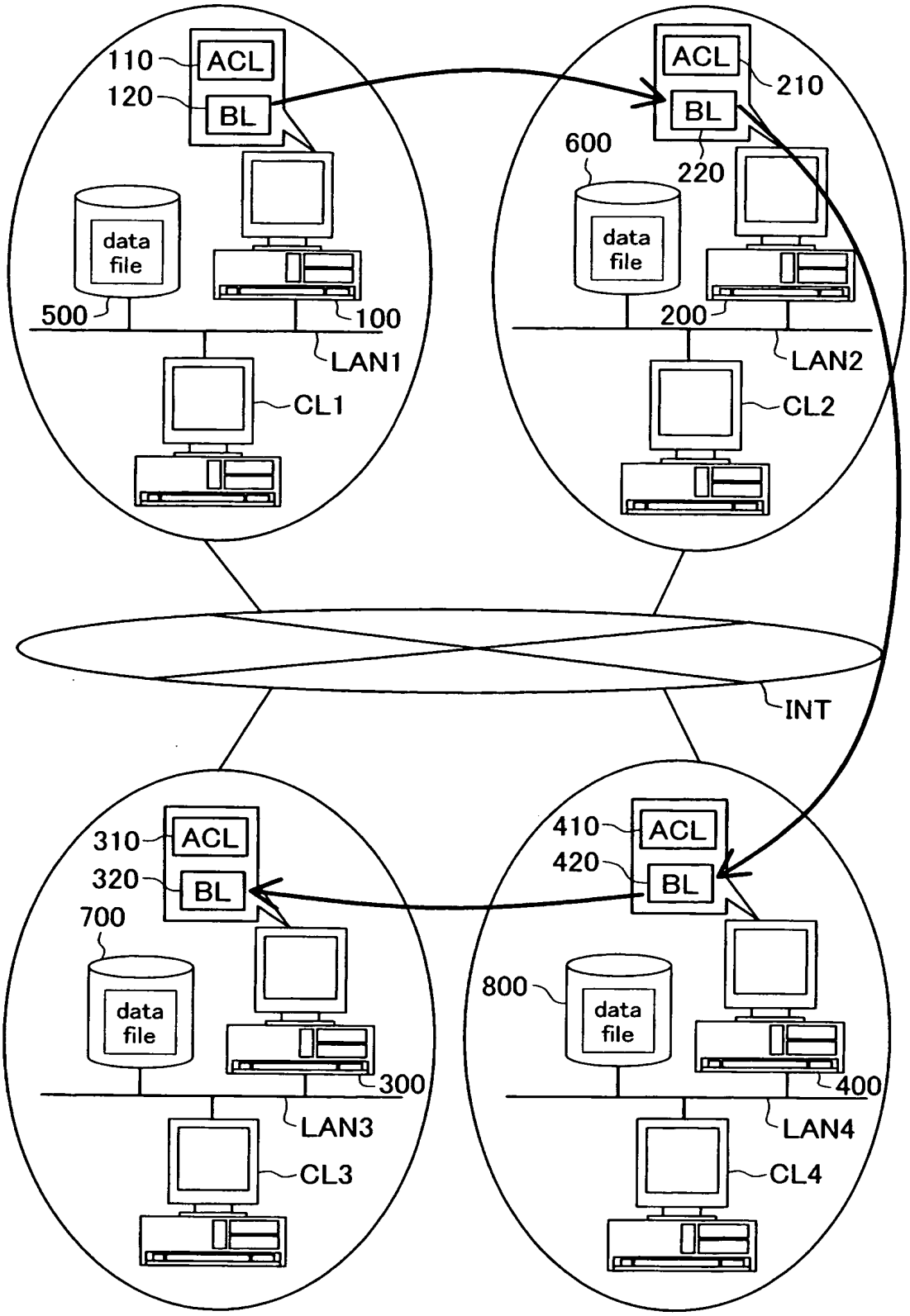
【図９】


ACL更新処理
S50
ブラックリストおよびACL参照
S51
グループ情報更新
G-1
G-2
S-1
S-2
S-5
S-4
S-3
G-1
G-2
S-2
S-5
S-4
S-3
S52
ブラックリストに登録されたユーザIDを削除
110
ID
オブジェクト
ユーザ
グループ
アクセス
1
0-1
S-3
—
R,W
2
0-1
—
G-1
R
3
0-2
S-7
—
R,W
4
0-2
—
G-3
R
5
6
0-3
—
G-2
R
END

【図１０】


アクセス制御装置 100
アクセス制御装置 200
アクセス制御装置 300
アクセス制御装置 400
Sa200
更新終了
Sa201:終了通知送出
Sa202
更新終了
Sa203:終了通知送出
Sa204
更新終了
Sa205:終了通知送出
Sa206
他のアクセス制御装置
全てからの更新終了通知受信
Sa207
削除
Sa208:ブラックリスト削除指示送出
Sa209
削除
Sa210:ブラックリスト削除指示送出
Sa211
削除
Sa212:ブラックリスト削除指示送出
Sa213
削除
END
END
END
END

【図１１】


110
ACL
120
BL
data file
500
100
LAN1
CL1
ACL
210
BL
600
220
data file
200
LAN2
CL2
INT
310
ACL
320
BL
700
data file
300
LAN3
CL3
410
ACL
420
BL
800
data file
400
LAN4
CL4

【書類名】要約書
【要約】
【課題】　超分散環境において、緊急アクセス遮断を実現する。
【解決手段】　アクセス制御装置１００は、オブジェクトのアクセス権限が設定されたアクセスコントロールリスト１１０（ＡＣＬ１１０）と、緊急アクセス遮断対象のユーザ情報が登録されたブラックリスト１２０（ＢＬ１２０）とを管理している。アクセス制御装置１００は、アクセス権限確認要求を受け、ＡＣＬ１１０に先立ちＢＬ１２０でアクセス許否を判断し、ＢＬ１２０でアクセス拒否されていない場合にはＡＣＬ１１０でアクセス許否を判断する。アクセス制御装置１００は、アクセス遮断対象のユーザ情報を他のアクセス制御装置に、各ブラックリストへの登録指示とともに配信する。本発明により、超分散環境において、緊急アクセス遮断を必要とするユーザが発生した場合にも、全てのネットワークで効率的に緊急アクセス遮断を行うことができる。
【選択図】　図１

特願２００３－３８９２３０

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所